C L A I M S

1. A security token comprising:

A Random Access Memory (RAM),

An Electrical Erasable Programmable Read Only Memory (EEPROM),

One or more Microprocessors, and

A Read Only Memory,

And characterized in that said EEPROM having at least an object containing a user certificate and an object containing a certificate of the certification authority (CA) of said user certificate (root certificate), wherein said root certificate is being write protected, and a verification component for checking authentication of said user certificate using information of said root certificate.

2. A security Token according to claim 1, wherein said user certificate comprises at least following information:

A name of issuer,
An identfier (ID) of said issuer,
A user identifier (ID),
A HASH algorithm,
A signature algorithm,
A public key, and

A digital signature.

3. A security token according to claim 1, wherein said root certificate comprises at least following information:

A certification authority name,
A certification authority identification (ID),
A HASH algorithm,
A signature algorithm,
A public root key, and
A digital signature.

4. Security Token according to claim 1 comprising the following further objects in said EEPROM:

A public root key,
A user's public key, and
A user's private key.

5. A security token according to claim 1, wherein said verification component is part of the operating system of said security token.

6. A seurity token according to claim 1, wherein said security token is a smart card.

7. A method for initializing a security token comprising the following steps:

a) transferring a root certificate of a certification authority into said security token using a secure transmission environment,

b) securing the root certificate against modifications , and

c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate.

8. A method according to claim 7, further comprising:

d) storing public root key additionally to said root certificate.

9. A method for authenticating information generated by an application using a security token according to claim 1 comprising the steps of:

a) retrieving a public root key from said root certificate,

b) generating a HASH over a user certificate using the HASH algorithm specified in said user certificate,

c) retrieving and decrypting a digital signature contained in said user certificate by applying said public root key resulting in a HASH of said user certificate, and

d) allowing use of said user certificate for signing said information with said digital signature when both HASHs are identical.

10. A method according to claim 9, wherein said information is a document or electronic mail.

11. A method according to claim 9, wherein said user certificate and said root certificate are sent to said application system and said steps a)-d) are accomplished on said application system.

12. A method according to claim 9, further comprising the step of:

checking the validity of the root certificate before retrieving said public root key.

13. A method for replacing a user certificate stored in a security token according to claim 1 comprising the steps of:

a) receiving a new user certificate from the certification authority and storing it into said EEPROM of said security token as a temporary object,
b) generating a HASH over a new user certificate using a HASH algorithm specified in said new user certificate,
c) retrieving a digital signature contained in said new user certificate and decrypting said digital signature by applying a public root key retrieved from a root certificate resulting in a HASH of said user certificate, and
d) permanently storing said new user certificate when both HASHs are identical.

14. Client-Server system having a client with a security token according to claim 1 to 6.

15. Data processing system using a security token according to claim 1 to 6.

16. Computer program product stored on a computer-readable media containing software for performing of the method according to claims 7 to 13.